Samordningsförbundet i Kalmar län

Riktlinje för personuppgiftsbehandling

Syfte och omfattning

Samordningsförbundet i Kalmar län har ett övergripande ansvar att inte bara följa dataskyddsförordningen utan även att visa hur organisationen ska göra detta, detta kallas i dataskyddsförordningen för ansvarsskyldighet. Detta innebär att Samordningsförbundet ska ta fram och följa dokumenterade planer för hur dataskyddsförordningen ska åtlydas. Denna riktlinje med instruktioner för personuppgiftsbehandlingen i Samordningsförbundet är utgångspunkten för Samordningsförbundets ansvarsskyldighet.

Ansvar

Samtliga inom organisationen.

Ändringshistorik

Datum	Ändring	Utförd av

PERSONUPPGIFTSANSVARIG

Personuppgiftsansvarig är den juridiska personen Samordningsförbundet. Styrelsen är ytterst ansvarig för organisationens behandling av personuppgifter.

BAKGRUND

Samordningsförbundet behandlar personuppgifter för att utföra de uppdrag organisationen har. Samordningsförbundets uppdrag följer av lag, förordningar, föreskrifter och politiska beslut.

Samordningsförbundet behandlar personuppgifter från och med den 25 maj 2018 i enlighet med dataskyddsförordningen och därtill hörande lagstiftning. I detta dokument redogörs principerna för hur personuppgifter ska behandlas inom Samordningsförbundets verksamheter.

PRINCIPER FÖR BEHANDLING AV PERSONUPPGIFTER

När personuppgifter behandlas (all hantering av personuppgifter utgör behandling) i Samordningsförbundet, eller på uppdrag av Samordningsförbundet, ska de grundläggande principerna i dataskyddsförordningen vara uppfyllda. Principerna anges i artikel 5 i dataskyddsförordningen och presenteras nedan.

Princip om laglighet, korrekthet och öppenhet

Personuppgifter ska behandlas på ett lagligt, korrekt och öppet sätt i förhållande till den registrerade. Med detta menas att Samordningsförbundet alltid ska vara tydlig och konkret i sin beskrivning av hur personuppgifter behandlas. Samordningsförbundet ska alltid se till att personuppgifter behandlas med stöd av en utpekad laglig grund och att annan lagstiftning som inverkar på informationen efterlevs. Regionen ska alltid ha avvägningen mellan den registrerades integritet och den egna verksamhetens effektivitet i åtanke. Registrerad ska ges möjlighet till insyn i hanteringen när sådan kan ske på ett pedagogiskt sätt och uppgifter ska alltid hanteras med hänsyn tagen till den registrerades integritet.

Princip om ändamålsbegränsning

Uppgifter ska samlas in för särskilda, uttryckligt angivna och berättigade ändamål och inte senare behandlas på ett sätt som är oförenligt med dessa ändamål.
Med detta menas att Samordningsförbundet hela tiden känner till och dokumenterar anledningen till att en viss personuppgift hanteras och personuppgifterna inte används för en helt annan anledning som går emot den ursprungliga.

Princip om uppgiftsminimering

Uppgifter ska vara adekvata, relevanta och inte för omfattande i förhållande till de ändamål för vilka de behandlas.
Med detta menas att Samordningsförbundet endast ska använda sig av de personuppgifter som krävs för att uppnå målet med hanteringen. Kan samma mål uppnås genom att använda färre personuppgifter eller mindre känsliga sådana ska så ske.

Princip om korrekthet

Uppgifter ska vara korrekta och om nödvändigt uppdaterade. Åtgärder måste vidtas för att säkerställa att personuppgifter som är felaktiga raderas eller rättas utan dröjsmål.
Med detta menas att Samordningsförbundet alltid måste verka för att personuppgifter som är felaktiga rättas och att det finns rutiner för hur så ska ske.

Princip om lagringsminimering

Uppgifter får inte förvaras identifierbara under en längre tid än vad som är nödvändigt för de ändamål för vilka personuppgifterna behandlas. Med detta menas att personuppgifterna inte får sparas längre än vad som behövs utifrån målet med behandlingen. När målet är uppnått ska gallring eller avidentifiering av personuppgifterna alltid övervägas med beaktande av de bevarande- och gallringsregler som gäller för Samordningsförbundet.

Princip om integritet och konfidentialitet

Personuppgifter ska behandlas på ett sätt som säkerställer lämplig säkerhet för uppgifterna, inbegripet skydd mot obehörig eller otillåten behandling och mot förlust, förstöring eller skada genom olyckshändelse, med användning av lämpliga tekniska eller organisatoriska åtgärder.
Med detta menas att personuppgifter ska skyddas genom tekniska och organisatoriska åtgärder på en nivå som motsvarar uppgifternas skyddsvärde. Är uppgifterna av särskilt skyddsvärd art ska också högre tekniska och organisatoriska krav ställas. Utgångspunkten ska alltid vara att endast behöriga personer ska ges tillgång till skyddsvärd information.

Princip om ansvarsskyldighet

Den personuppgiftsansvarige ska ansvara för och kunna visa att de nu nämnda grundläggande principerna enligt dataskyddsförordningen efterlevs.
Med detta menas att Samordningsförbundet inte bara ska uppfylla dessa principer utan också på ett öppet och tillgängligt sätt demonstrera på vilket sätt så sker.

DATASKYDDSFÖRORDNING OCH OFFENTLIGHETSPRINCIPEN

Offentlighetsprincipen innebär en rätt för var och en att hos Samordningsförbundet ta del av allmänna handlingar. Detta innebär att även personuppgifter kan begäras och lämnas ut som en del av allmän handling oavsett för vilket ändamål personuppgiften ursprungligen behandlades.
Denna rätt gäller dock inte om handlingarna innehåller uppgifter som omfattas av sekretess enligt offentlighets- och sekretesslagen (2009:400). Sekretess enligt offentlighets- och sekretesslagen gäller bland annat för personuppgift om det kan antas att ett utlämnande skulle medföra att personuppgiften behandlas i strid med dataskyddsförordningen eller dataskyddslagen.

RÄTTSLIG GRUND

All behandling av personuppgifter som Samordningsförbundet utför måste vila på minst en rättslig grund, i annat fall är behandlingen olaglig.
Detta innebär att organisationen måste ha klart för sig vilken eller vilka rättslig grund(er) som är tillämplig för varje specifik behandling av personuppgifter redan när denna behandling påbörjas. De rättsliga grunder som finns tillgängliga framgår av dataskyddsförordningen artikel 6; En sådan rättslig grund är *samtycke från* den registrerade. Andra rättsliga grunder är om personuppgiftsbehandlingen är nödvändig för att fullgöra *ett avtal* med den registrerade, fullgöra en *rättslig förpliktelse*, skydda den registrerades *grundläggande intressen*, fullgöra en *uppgift av allmänt intresse*, för *myndighetsutövning*, samt efter *berättigat intresse* (s.k. intresseavvägning).
Samordningsförbundet utför i egenskap av myndighet uppgifter av allmänt intresse och det är därför primärt denna rättsliga grund samt att fullgöra en rättslig förpliktelse som regionen baserar sin behandling av personuppgifter på. Den rättsliga grunden berättigat intresse (intresseavvägning) får inte användas av myndigheter när de utför sina uppgifter och ska därför som huvudregel inte användas av Samordningsförbundet.

KÄNSLIGA PERSONUPPGIFTER

Vissa personuppgifter är till sin natur mer känsliga än andra. I dataskyddsförordningen anses följande särskilda kategorier av personuppgifter kräva ett särskilt legalt skydd. Ras eller etniskt ursprung, politiska åsikter, religiös eller filosofisk övertygelse, medlemskap i en fackförening, hälsa, en persons sexualliv eller sexuella läggning, genetiska uppgifter och biometriska uppgifter som entydigt identifierar en person.
Samordningsförbundet ska endast behandla känsliga personuppgifter när det finns särskilt stöd i lag eller om den registrerade särskilt samtyckt till den specifika behandlingen. Det här innebär att varje gång känsliga personuppgifter ska användas av Samordningsförbundet måste en särskild bedömning ske om att hanteringen verkligen är tillåten och att den sker på ett säkert sätt. Känsliga personuppgifter ska alltid ges ett högt skydd mot obehörig åtkomst.

SKYDDSVÄRDA PERSONUPPGIFTER

Även personuppgifter som inte är särskilt reglerade som känsliga kan vara mer skyddsvärda än andra. Personuppgifter av mycket personlig eller privat natur anses generellt vara mer skyddsvärda än andra typer av personuppgifter. Så gör även personuppgifter som möjliggör samkörning mellan register som t.ex. personnummer eller andra samordningsnummer. Det här innebär att Samordningsförbundet alltid ska bedöma om de personuppgifter som behandlas är särskilt skyddsvärda mot bakgrund av sin privata natur, sin mängd eller av annan anledning. Denna bedömning har betydelse för valet av nivå för skyddsåtgärder.

Särskilt vad gäller personnummer

Personnummer och samordningsnummer ska enligt dataskyddslagen endast hanteras om det är klart motiverat med hänsyn till ändamålet med behandlingen, vikten av en säker identifiering eller något annat beaktansvärt skäl.
Det här innebär att Samordningsförbundet alltid ska bedöma om personnummer är en nödvändig del av en behandling av personuppgifter och alltid överväga om ändamålen kan uppfyllas utan att personnummer används.

REGISTER ÖVER BEHANDLINGAR

Samordningsförbundet ska, enligt dataskyddsförordningen artikel 30, föra ett register över behandlingar av personuppgifter som utförs under organisationens personuppgiftsansvar. Det här innebär att Samordningsförbundet ska ha en vid var tid gällande förteckning över samtliga behandlingar (IT-stöd innehållande personuppgifter, regionala och lokala register, processer eller andra typer av behandlingar) som sker. Denna förteckning ska upprättas skriftligt, vara tillgänglig i elektronisk format och hållas uppdaterad. På begäran ska registret göras tillgängligt för tillsynsmyndigheten.

Ansvarig för respektive behandling ska innan behandlingen påbörjas anmäla behandlingen. Anmälan görs i Samordningsförbundets registerförteckning. Den som genomfört anmälan är även ansvarig för att den anmälda behandling uppdateras när nya förutsättningar gäller för dess hantering, såsom t.ex. att den avslutats eller att de informationssäkerhetsmässiga skydden förändrats.
Samordningsförbundet för även ett register över behandlingar av personuppgifter där Samordningsförbundet agerar som personuppgiftsbiträde åt en annan personuppgiftsansvarig. Den som organisatoriskt ansvarar för beslutet att Samordningsförbundets behandlar personuppgifter för någon annans räkning ska innan behandlingen påbörjas anmäla behandlingen till Samordningsförbundets personuppgiftsbiträdesförteckning.

ÖVERFÖRING AV PERSONUPPGIFTER UTANFÖR EU/EES

Huvudregeln i Samordningsförbundet är att ett förbud råder mot att föra ut personuppgifter utanför EU/EES.
Enligt dataskyddsförordningen är överföring av personuppgifter utanför EU/EES endast tillåtet under vissa omständigheter. För överföring av personuppgifter till ett land utanför EU/EES krävs att landet uppfyller dataskyddsförordningens och EU-kommissionens krav på s.k. adekvat skyddsnivå för personuppgifter eller att EU-kommissionens standardavtalsvillkor används vid avtalsskrivandet med leverantören. För överföring av personuppgifter till USA kan det annars räcka att den mottagande leverantören är ansluten till villkoren i Privacy Shield.
En överföring av personuppgifter utanför EU/EES får endast genomföras om Samordningsförbundet bedömer att tillräckliga garantier givits om att personuppgifterna kommer att hanteras på ett säkert sätt.

ANVÄNDANDE AV PERSONUPPGIFTSBITRÄDE

Samordningsförbundet ska endast använda sig av personuppgiftsbiträde för sin behandling av personuppgifter om det anlitade personuppgiftsbiträdet ger tillräckliga garantier att skydda personuppgifter genom såväl tekniska som organisatoriska åtgärder. Nivån på skyddet ska överensstämma med den nivå som enligt Samordningsförbundets bedömning krävs för att behandlingen ska uppfylla dataskyddsförordningens krav och för att säkerställa att de registrerades rättigheter skyddas.

Personuppgiftsbiträde får inte anlita ett annat personuppgiftsbiträde (s.k. underbiträde) utan att ett särskilt eller allmänt skriftligt förhandstillstånd har erhållits från Samordningsförbundet. Om ett sådant allmänt skriftligt tillstånd har erhållits, ska personuppgiftsbiträdet löpande informera Samordningsförbundet om eventuella planer på att anlita eller ersätta personuppgiftsbiträden, så att Samordningsförbundet har möjlighet att göra invändningar.
När personuppgiftsombud anlitas ska ett biträdesavtal (pub-avtal) tecknas mellan biträdet och Samordningsförbundet. Biträdesavtalet ska undertecknas av den som har behörighet enligt gällande delegationsordning.
Samordningsförbundet kan agera som personuppgiftsbiträde åt en personuppgiftsansvarig. Om Samordningsförbundet agerar som personuppgiftsbiträde åt en personuppgiftsansvarig ska ett biträdesavtal tecknas mellan den personuppgiftsansvarige och Samordningsförbundet.

SÄKERHETSÅTGÄRDER

Samordningsförbundet har ett ansvar för att ha en lämplig säkerhetsnivå för hantering av personuppgifter, både tekniskt och organisatoriskt. Vad som är en lämplig säkerhetsnivå beror på bland annat riskerna med behandlingen, vilken typ av uppgifter som behandlas, på de tekniska möjligheter som finns och på kostnaderna. Det här innebär att Samordningsförbundet måste ta ställning till vilka risker som finns och vilka säkerhetsåtgärder dessa risker motiverar. Detta sker genom informationsklassificering och riskanalys.

Särskilt om informationsklassificering och riskanalys

Ovanstående innebär att Samordningsförbundet alltid ska genomföra en organiserad och dokumenterad bedömning av vilka säkerhetsåtgärder som krävs för en viss typ av behandling. Sådan bedömning ska ske på ett systematiskt sätt inom ramen för Samordningsförbundets arbete med informationssäkerhet. Tidigare genomförda riskanalyser kan ligga till grund för nya behandlingar av samma art.

Konsekvensbedömning

Om en behandling av personuppgifter som kan leda till en hög risk för de registrerade (t.ex. en omfattande hantering av känsliga personuppgifter eller risk att särskilda krav avseende skydd inte kommer att kunna uppnås) planeras att genomföras ska Samordningsförbundet enligt dataskyddsförordningen först genomföra en så kallad konsekvensbedömning avseende dataskydd. Om en sådan konsekvensbedömning innebär att de bedömda höga riskerna kvarstår ska Samordningsförbundet samråda med tillsynsmyndigheten (Integritetsskyddsmyndigheten) innan behandlingen påbörjas.

INFORMATION OCH KOMMUNIKATION

Samordningsförbundet ska tillhandahålla information till registrerad i enlighet med dataskyddsförordningens krav. Informationen ska ges om hur Samordningsförbundet behandlar de registrerades personuppgifter och om vilka rättigheter som de registrerade har enligt dataskyddsförordningen.
Information som ges ska vara koncis, klar, tydlig och begriplig och den ska ges i ett lättillgängligt format. Språket ska vara klart och tydligt, och vara anpassat till mottagaren, exempelvis om informationen är särskilt riktad till barn.
Informationen ska tillhandahållas skriftligt och kan när det är lämpligt ges i elektronisk form. Om den registrerade begär det ska informationen tillhandahållas muntligt, under förutsättning att den registrerade har styrkt sin identitet. Det här innebär att den som ansvarar för behandlingen alltid måste ta ställning till om den information som krävs kan anses omfattas av någon av de centralt givna informationerna till registrerade (som ”så behandlas dina

personuppgifter i Samordningsförbundet). Om så inte bedöms vara fallet måste de registrerade informeras särskilt.

DEN REGISTRERADES RÄTTIGHER

Alla registrerade har rättigheter gentemot den som är personuppgiftsansvarig. Vissa av rättigheterna är beroende av vilken rättslig grund som den aktuella behandlingen av personuppgifter vilar på. Detta innebär att vissa rättigheter bara kan göras gällande under vissa förutsättningar. Samordningsförbundet ska möjliggöra för de registrerade att utöva sina rättigheter.

Rätt till insyn och registerutdrag

Den registrerade har rätt att få tillgång till de personuppgifter som behandlas. Detta innebär att Samordningsförbundet på begäran måste kunna tillhandahålla dessa uppgifter till den registrerade. Denna process benämns inom Samordningsförbundet för ett registerutdrag.

Rätt till ändring

Den registrerade har rätt att begära att felaktiga personuppgifter rättas och att ofullständiga personuppgifter kompletteras.

Rätt till radering, rätten att bli glömd

Beroende på omständigheter i det enskilda fallet och vilken rättslig grund som personuppgiftsbehandlingen görs kan den registrerade även ha rätt till radering av sina personuppgifter. Rättigheten har begränsad tillämpning inom offentlig förvaltning eftersom merparten av personuppgiftsbehandlingarna vilar på en rättslig grund där rättigheten inte är tillämplig.

Rätt till begränsning

Beroende på omständigheter i det enskilda fallet kan den registrerade ha rätt till att behandlingen av personuppgifterna begränsas till endast lagring under den tid det tar att utreda en invändning från den registrerade.

Rätt till dataportabilitet

Beroende på omständigheter i det enskilda fallet och på vilken rättslig grund som personuppgiftsbehandlingen grundar sig på har den registrerade i vissa fall rätt att få tillgång till personuppgifterna i ett sådant format som möjliggör överförande till en annan personuppgiftsansvarig. Rättigheten har begränsad tillämpning inom offentlig förvaltning eftersom merparten av personuppgiftsbehandlingarna vilar på en rättslig grund där rättigheten inte är tillämplig.

Återkallande av samtycke

Om den rättsliga grunden för en behandling av personuppgifter är ett samtycke från den registrerade så har denne rätt att återkalla samtycket. Ett återkallande av samtycket påverkar dock inte lagligheten av personuppgiftsbehandlingen för tiden innan samtycket återkallades.

Invända mot behandling

Om den lagliga grunden för behandlingen av personuppgifter baseras på berättigat intresse (intresseavvägning) eller allmänt intresse har registrerade under vissa förutsättningar rätt att invända mot hur dennes personuppgifter behandlas. Det här innebär att den registrerade har rätt att ifrågasätta huruvida det finns ett allmänt intresse avseende den aktuella behandlingen och att Samordningsförbundet måste kunna motivera detta.

Rätt att lämna klagomål till tillsynsmyndigheten

Den registrerade har alltid rätt att vända sig till tillsynsmyndigheten med klagomål om denne inte är nöjd med hur Samordningsförbundet hanterar den registrerades personuppgifter. Tillsynsmyndighet är Integritetsskyddsmyndigheten.